Invoice Permissions Fix - Summary

Issue

Invoice receivers were unable to view their invoices due to a permissions error. The invoice list page was calling `getAll` query unconditionally, which required elevated permissions that receivers didn't have.

Root Cause

In `app/(dashboard)/(modules)/invoices/page.tsx`, both the `getAll` and `getMyInvoices` queries were being called with `enabled: true` unconditionally (lines 72-80):

```
const globalQuery = api.invoice.getAll.useQuery(
  { limit: 200 },
  { enabled: true }  // ❌ Always enabled
);

const ownQuery = api.invoice.getMyInvoices.useQuery(
  undefined,
  { enabled: true }  // ❌ Always enabled
);
```

This meant that even users with only `invoice.read.own` permission were attempting to fetch all invoices through the `getAll` endpoint, causing permission errors.

Solution

Updated the queries to be conditionally enabled based on user permissions:

```
const globalQuery = api.invoice.getAll.useQuery(
  { limit: 200 },
  { enabled: CAN_LIST_GLOBAL }  // ✅ Only for users with LIST_GLOBAL
);

const ownQuery = api.invoice.getMyInvoices.useQuery(
  undefined,
  { enabled: CAN_READ_OWN && !CAN_LIST_GLOBAL }  // ✅ Only for users with READ_OWN
(but not LIST_GLOBAL)
);
```

Benefits

1. **Proper Permission Enforcement**: Users only call endpoints they have permissions for
2. **Better Performance**: Reduces unnecessary API calls
3. **Security**: Prevents unauthorized data access attempts
4. **User Experience**: Invoice receivers can now view their invoices without errors

How It Works

- **Admin users** with `invoice.list.global` permission: Use `getAll` to see all invoices
- **Regular users/receivers** with `invoice.read.own` permission: Use `getMyInvoices` to see only their own invoices (created by them or received by them)
- The `getMyInvoices` endpoint already includes the logic to show invoices where the user is either the creator OR the receiver

Backend Support

The `getMyInvoices` endpoint in `server/api/routers/invoice.ts` (lines 118-158) already supports showing invoices where the user is involved:

```
getMyInvoices: tenantProcedure
  .use(hasPermission(P.READ_OWN))
  .query(async ({ ctx }) => {
    return ctx.prisma.invoice.findMany({
      where: {
        tenantId: ctx.tenantId,
        OR: [
          { createdBy: ctx.session.user.id },
          { receiverId: ctx.session.user.id },  // 🔥 Includes received invoices
        ],
      },
      // ...
    })
  }),
```

Commit Details

- **Commit**: `3633393edc632915bd53bc79f28f7a80df19ad8d`
- **Branch**: `expenses-structure`
- **Files Changed**: 1 file, 3 insertions(+), 3 deletions(-)
- **Date**: December 12, 2025

Testing Recommendations

1. Test with a user that has only `invoice.read.own` permission (invoice receiver)
2. Verify they can see invoices where they are the receiver
3. Test with an admin user to ensure they still see all invoices
4. Check that no permission errors appear in the console